

REMARKS

Applicants respectfully request reconsideration of the application.

In the Office Action, the Office raised objections to certain informalities in the specification and drawings. These have been addressed in the above amendments to the specification and drawings.

Claims 1-2 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,615,348 to Gibbs. In this rejection, the Office takes the position that a digital signature corresponds to a digital watermark. The term "watermark" as used in the specification refers to a method of carrying auxiliary data (such as a payload having fields and/or flags) in host data, such as a document, image or audio clip, by varying the host data to carry the auxiliary data. In contrast, Gibbs teaches that a digital signature is implemented as a hash function. Since Gibbs does not teach the watermark as claimed, it does not anticipate claims 1-2.

Claims 1-6 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,958,005 to Thorne et al. ("Thorne") in view of U.S. Patent No. 5,862,260 to Rhoads.

Claim 1, as amended, clarifies that the system detects watermarks in documents forming at least part of a message as well as documents attached to a message. Thorne and Rhoads, even when combined, do not teach all of the elements of claim 1. Even if Rhoads teachings were used to modify Thorne's system to replace headers with "bodiers" from Rhoads, the combined teachings still do not teach the claimed program for reading watermarks in documents that form at least part of the messages and documents attached to the messages.

Regarding claim 2, the combination of Thorne and Rhoads fails to disclose or suggest: "watermark detecting means for detecting and reading watermarks in e-mail messages at the server after the messages are sent from the user but before such messages are transmitted from said e-mail server to the Internet." The cited passages in Fig. 3 and accompanying text in Thorne refer to how the header data is set by the user before an email message is sent. This is clear in Fig. 3 where it shows the setting of the header occurs after opening the e-mail program to compose a message in step 302 and before the message is composed and sent in steps 327 and 328. The cited passages in Fig. 5A and accompanying text in Thorne refers to scanning of e-mail messages during an email retrieval procedure when the e-mail program is opened or closed. The

combination of Thorne and Rhoads does not teach the claimed detecting and reading means after messages are sent from a user to a server, but before the server transmits them to the Internet as claimed.

The combination of Thorne and Rhoads does not disclose, teach or suggest all of the elements of claim 3. Even if the header in Thorne is replaced by the body of Rhoads, the combination fails to disclose or suggest a mechanism for controlling the distribution of documents attached to messages as claimed.

Claim 4 is patentable for the same reasons as claim 3.

The combined teachings of Thorne and Rhoads fail to teach reading of watermarks in documents in and attached to messages as recited in claim 5.

Claim 6 is patentable for the same reasons as claim 5.

In rejecting claim 7, the Office contends that Kasiraj teaches comparing a message profile with a previously established profile, "inherently contained in a database." First, claim 7 has been amended to clarify that the database is interrogated to determine an action to take with a particular message based on the data carried by the watermark. The combined teachings of Thorne, Rhoads and Kasiraj fail to teach all of the elements of claim 7. In particular, Kasiraj does not suggest interrogation of a database as claimed. Kasiraj checks whether restrictions for a component match the recipient's profile or a profile transmitted with the message. Neither the profile of the message nor the profile of the recipient involve interrogation of a database as claimed.

Moreover, Kasiraj analyzes restrictions upon receipt of an electronic message as shown in Fig. 3 because the recipient's profile, retrieved from the recipient's system in block 42, is required for the analysis. In contrast, the claim describes an approach for controlling distribution prior to transmission. Therefore, the combined teachings of Kasiraj, Thorne and Rhoads fail to teach interrogation of a database based on data carried in a watermark as recited in claim 7, and the required motivation to combine these references is lacking.

The combined teachings of Kasiraj, Thorne and Rhoads fail to teach the elements of claim 8, and there is no motivation to combine these references because the recipient's profile is analyzed upon receipt of a message in contrast to the claim.

The combined teachings of the cited art fail to teach all of the elements of claim 9 because they fail to teach an action dependent on information carried by the watermark and information stored in a database as claimed. The motivation to combine these references is lacking as well.

Similarly for claim 10, the combined teachings of the cited art fail to teach all of the elements of claim 10 because they fail to teach how to interrogate a database to determine an action based on information carried by the watermark and information stored in a database as claimed. The motivation to combine these references is lacking as well. Claims 11 and 12 are patentable for the same reasons as claim 10.

New claims 13-16 include a combination of elements not disclosed, taught or suggested in the cited art.

Date: February 10, 2004

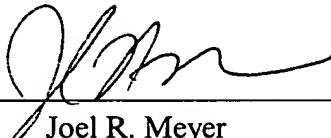
Customer Number 23735

Telephone: 503-885-9699
FAX: 503-885-9880

Respectfully submitted,

DIGIMARC CORPORATION

By



Joel R. Meyer
Registration No. 37,677